Cybercrimes in Nigeria: Analysis, Detection and Prevention

* B. A. Omodunbi, P. O. Odiase, O. M Olaniyan and A. O. Esan
Department of Computer Engineering, Federal University Oye Ekiti, Nigeria
bolaji.omodunbi@fuoye.edu.ng

Abstract— Over the years, the alarming growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria today, several internet assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. Cybercrime is a threat against various institutions and people who are connected to the internet either through their computers or mobile technologies. The exponential increase of this crime in the society has become a strong issue that should not be overlooked. The impact of this kind of crime can be felt on the lives, economy and international reputation of a nation. Therefore, this paper focuses on the prominent cybercrimes carried out in the various sectorsin Nigeria and presents a brief analysis of cybercrimes in tertiary institutions in Ekiti-State. In conclusion, detection and prevention techniques are highlighted in order to combat cybercrimes in Nigeria.

Keywords— Cybercrime, Phishing, Plagiarism, Security

1 Introduction

In recent times, our society is increasingly relying on the internet and other information technology tools to engage in personal communication and conduct business activities among other several benefits. While these developments allow for enormous gain in productivity, efficiency and communication they also create a loophole which may totally destroy an organisation. The term cybercrime can be used to describe any criminal activity which involves the computer or the internet network (Okeshola, 2013). This term is used for crimes such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used.

In (Maitanmi, 2013) cybercrime was defined as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. Cybercrime evolves from the wrong application or abuse of internet services. The concept of cybercrime is historical. It was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960s (Maitanmi, 2013). Since these computers were not connected to the internet or with other computers, the crime was committed by the employers (insider) in the company, hence it was referred to as computer crime rather than cybercrime.

According to (Lakshmi, 2015) as at 2003, the United States and South-Korea have the highest cyber-attacks of 35.4% and 12.8% respectively. With the population of Nigeria placed at 160 million from the last census carried out in 2006, a recent statistics revealed that about 28.9% have access to the internet(Hassan, 2012). It was also proven that 39.6% African users of internet are actually Nigerian, hence, the high increase in the rate of internet crime in Nigeria (Hassan, 2012). Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young. Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young.

2 Overview of Cybercrime

Cybercrime is a new trend that is gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. The crime usually requires a hectic task to trace. Generally, cybercrime may be divided into one of two types of categories:

1. Crimes that affects computer networks and devices directly. Examples are malicious code, computing viruses, malware etc.
2. Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Cyber Stalking, Fraud and identity theft, phishing scams and information warfare.

2.1 Causes of Cybercrimes in Nigeria

The following are some of the identified causes of cybercrime (Hassan, 2012)

a. Unemployment is one of the major causes of Cybercrime in Nigeria. It is a known fact that over 20 million graduates in the country do not have gainful employment. This has automatically increased the rate at which they take part in criminal activities for their survival.

b. Quest for Wealth is another cause of cybercrime in Nigeria. Youths of nowadays are very greedy, they are not ready to start small hence they strive to level up with their rich counterparts by engaging in cybercrimes.

c. Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.

d. Incompetent security on personal computers. Some personal computers do not have proper or competent security controls, it is prone to criminal activities hence the information on it can be stolen.

.

2.2 Various Cybercrimes in Nigeria

Over the past decade, the internet has experienced an explosive growth with the number of hosts connected to the internet increasing daily at an exponential rate. As the internet grows to become more accessible and more services become reliant on it for their daily operation, so does the threat landscape. In Nigeria, cybercrime has become one of the main

* Corresponding Author

avenues for pilfering money and business espionage. According to Check Point, a global network cyber security vendor, as of 2016, Nigeria is ranked 16th highest country in cyber-attacks vulnerabilities in Africa (Ewepu, 2016). Nigerians are known both home and abroad to be rampant perpetuators of cybercrimes. The number of Nigerians caught for duplicitous activities carried by broadcasting stations are much more in comparison to other citizens of different countries. The contribution of the internet to the development of Nigeria has had a positive impact on various sectors of the country. However, these sectors such as the banking, e-commerce and educational sector battles with the effect of cybercrimes. More cybercrimes are arising at an alarming rate with each subsequent crime more advanced than its predecessor. Therefore, in this section, prominent specific ways in which cybercrimes are mostly carried out in Nigeria are discussed.

2.3 Cybercrimes in the Banking Sector

The life wire of the banking sector is the internet. Currently, banks all over the world are taking advantage and incorporating opportunities brought about by e-banking which is believed to have started in the early 1980's (Shandilya, 2011). As the security level in this sector becomes stronger, the strength and tactics of these fraudsters increases also. Various lucrative attacks have been launched and unfortunately, many have succeeded. In general, cybercriminals execute fraudulent activities with the ultimate goal of accessing a user's bank account to either steal or/and transfer funds to another bank account without rightful authorisation. However, in some rare cases in Nigeria, the intention of cybercriminals is to cause damage to the reputation of the bank by denying service to users (Parthiban, 2014) and sabotaging data in computer networks of organizations.

Bank Verification Number (BVN) Scams: The BVN is a biometric identification system which consists of an 11-digit number that acts as a universal ID across all the banks in Nigeria. BVN was implemented in 2015 by the Central Bank of Nigeria. It was introduced to link various accounts to the owner thereby ensuring that fraudulent activities are minimised. For fraudsters, opportunities to extort money and to carry out other fraudulent activities arose from the implementation of the BVN. It was detected that fake and unauthorised text messages and phone calls were sent to various users demanding for personal information such as their account details. In addition, phishing sites were created to acquire such information for insalubrious activities on the bank account.

Phishing: Phishing is simply the theft of an identity. It involves stealing personal information from unsuspecting users and it is also an act of fraud against the authentic, authorised businesses and financial institutions that are victimized (Wada). Phishing scams are ubiquitous and are exponentially increasing. It has become one of the fastest growing cybercrimes in Nigeria. In this jet age of technology, hoi polloi subscribe to a plethora of sites using their email addresses and are therefore expecting to receive mails of updates of their membership or subscription. So it seems natural when users get regular mails from such organizations. Fraudster have devised a means to mimic authorised organisations and retrieve confidential information from clients. In Phishing email messages, the fraudsters find a way to convince and gain the trust of users. An instance of such mail is shown in the figure below showcasing a fraudster trying to build the trust of a client in order to convince them to give up personal banking information. In Nigeria, phishing mails are mostly carried out on bank customers.

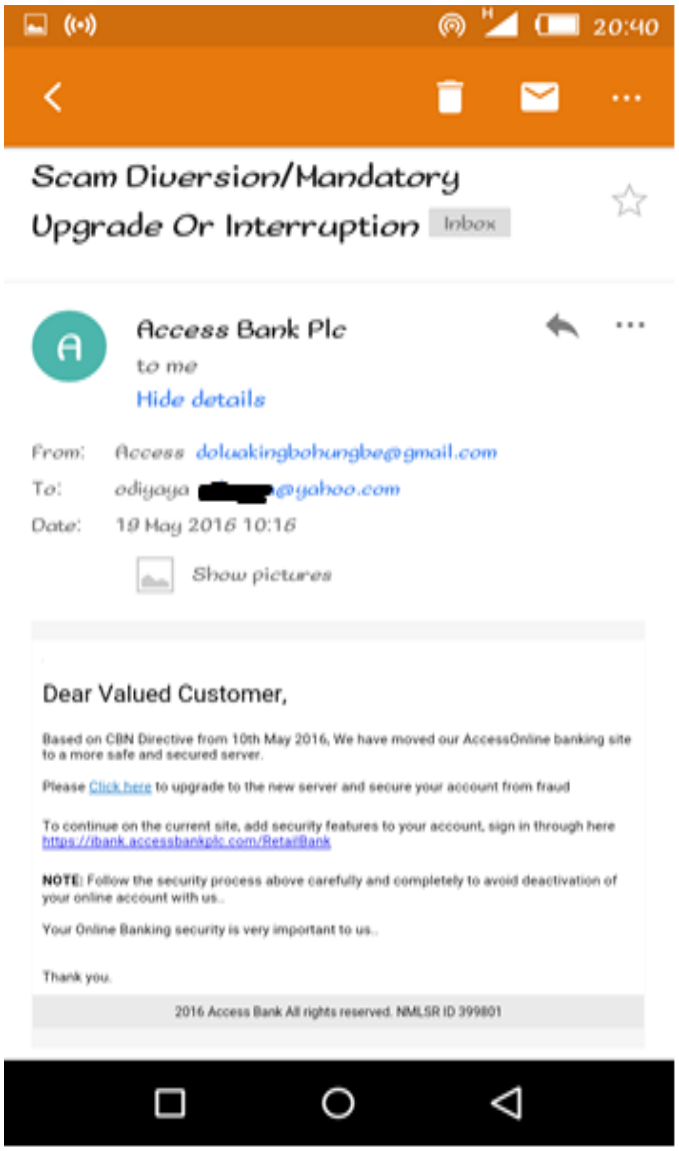


Fig 1. Phishing e-mail message

Theft of Bank Cards: The theft of bank cards has evolved from the physical theft of the card to simply the theft of the numbers. Today, bank card hackers do not need to be in the same country to steal other people's identities. Fraudsters make use of hidden cameras to record ATM card pins and numbers in distinct places such as an eatery payment using POS, or at the ATM. According to the Federal Bureau of Investigation (FBI), a method known as ATM skimming can be used and it involves placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine (FBI, 2011). Also, another cybercrime carried out via this means in Nigeria includes internet order fraud. Internet order frauds involves fraudster inputting stolen cards numbers on online commer-

cial sites to order goods. Credit card numbers or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction. Different applications can be used to retrieve this information such as key loggers at cybercafés or cloned websites.

Cyber-theft / Banking Fraud: Hackers target the vulnerabilities in the security of various bank systems and transfer money from innumerable accounts to theirs. Most cybercriminals transfer bantam amounts like 5 naira which are sometimes overlooked by the user without questions raised by the users who assumes this was deducted for either SMS or ATM withdrawal charges. Doing this for over a million accounts enriches most fraudsters.

2.4 Cybercrimes in the e-Commerce Sector

The Nigerian economy, including the enormous amount of e- businesses, is greatly threatened by the rapid increase of e-crimes. E-commerce refers to the use of technology, particularly the Internet, to buy, sell and market goods and services to customers (Michael, 2014). Very few e-crimes are discovered in this sector because most businesses fear the loss from negative publicity than the crimes involved. In a recent article by This Day and Vanguard, Senator Iroegbu estimated the annual cost of cybercrime to Nigeria at about 0.08% of the county's Gross Domestic products (GDP) which amounts to approximately 127 billion Naira (Ewepu, 2016).

Software Piracy (Intellectual Property Theft): The term "Copyright" means little or nothing to the average Nigerian. Piracy involves the unlawful reproduction and sharing of applications software, games, movies/videos and audios. Cybercriminals make money from the illegal sales of pirated copies of software and even go as far as providing cracks for pirated software. The internet has created a platform for almost anonymous, free and illegal distribution of pirated materials in Nigeria.

Sales Fraud & Forgery: In our society today, fraudulent sales of products that do not exist or that are replicas are increasingly common. The purchase of an item before actually seeing it has created ways for fraudsters to make money via the sale of unoriginal products or in some cases, the total absence of the product. Many persons have fallen victim of this particular crimes on popular e-commerce websites.

Data and Airtime Time (DAT) theft from service providers: This is a very rampant scam among the youths of today. They illegally gain access to "Cheat codes" and unlawfully use them to gain thousands of mobile data and unlimited airtime without making the necessary payment. Also, cyber cafes have developed means of connecting to the network of internet service providers.

2.5 Cybercrimes in the Education Sector

The educational sector in Nigeria suffers greatly from electronic crimes which are perpetuated mostly by students in tertiary institutions.

Cyber-Plagiarism: Information housed on the internet has made an effective alteration on the methods in which people educate themselves. The term 'Copy and Paste' is the most common phrase used when referring to cyber-plagiarism. Cyber-plagiarism can be defined as copying and pasting online sources into word processing documents without reference to the original writer /owner. In the educational sector in Nigeria, students, particularly those in the tertiary institutions carry out this crime without enforcing the due penalty.

Cyber-Pornography*:* Cyber-pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyber-pornography is a criminal offense, classified as causing harm to persons.

2.6 Cybercrimes on Social Media Sector

In Nigeria, Social networks have gained a very high ground in every sector. The banking industry, government, business, universities use this platform to promote and communicate with each other. Social networking sites such as Facebook, Twitter, LinkedIn and Instagram serve as a fertile ground for cybercriminals to launch new attacks. Users create semi-public profiles and can directly communicate with friends without restriction (Michael, 2014).

Nigerian-Prince (Beneficiary of a will) Scam: The fraudsters send messages via social media sites speculating that the receiver is a named beneficiary of a huge some of amount or an estate from a will left behind from a deceased descendant.

Charity Funds: Fraudulent people host fake social network pages for charity soliciting for money. In most cases, these fake social pages are backed up with pictures showcasing various illnesses. Many kind hearted people donate to this cause thereby increasing the pockets of cyber criminals.

Cyber-Stalking, harassment and Blackmailing Scam: Threatening and blackmailing acts carried out on the internet by fraudsters on the victim. In most cases, the perpetuator's identity is unknown by the use of a false alias or by blocking the identity by keeping all information hidden.

Social-Hi-Jacking: This is a major crime all over the world. Many social networking pages have been hi-jacked by hackers who demands money in turn for releasing the personal social page. This has occurred in sites like Twitter, Facebook and Instagram. These fraudsters go as far as sending messages from the authorised page to friends and family requesting for money or any other kind of assistance. Also, another common scenario also occurs when the fraudster creates a social page pretending to be someone else especially celebrities.

2.7 Detection of Cybercrime

The following are some of the ways by which cybercrimes can be detected (Okeshola, 2013).

Email inspection: inspecting your mails before opening is a very useful way of detecting unusual or strange activities. Email spamming and cyber stalking can be detected by carefully investigating the email header which contains the real email address, the internet protocol address of the sender as well as the date and time it was sent.

Constant reviewing to detect mistakes: It has been discov-

ered that cyber criminals can get very careless; hence it is advisable to review the system regularly to discover unusual mistakes.

Use of network intrusion detection system: this is applicable for more serious attacks like breaking into a bank network to steal customers sensitive data which cannot be discovered by mere inspection or reviewing. Intrusion detection techniques such as Honey pots, Tripwires, Anomaly detection systems, Operating system commands and Configuration checking tools are always employed.

Another well-known system is Snort, it is arobust open source tool which exist for monitoring different network attacks (Ndible, 2016). It was first developed in 1998 and gradually evolved into a mature software and even better than many commercial IDS. The system employs the rules established by the administrator to monitor traffic and detect strange behaviours.

2.8 Detection of Cybercrime

Cybercrime cannot be easily and completely wiped out, but can be reduced. However, collaborative efforts of individuals alongside with government intervention could go a long way to minimise it to a reasonable level. Measures to take can be categorised into two (Maitanmi, 2013):

a) Governments intervention: Although the country has found herself in great mess by the inability of the government to provide basic necessary amenities such as jobs, security and the likes for her citizens which indirectly has led to high rate in cybercrime, there is still need for the nation to come up with adequate laws to tackle this issue. These laws should be formulated by the government and should strictly be adhered to. However, it is worthy to note that a bill was recently passed in year 2015 that would protect and punish electronic fraud and other cyber related crimes. The full implementation of this bill will hopefully bring a strategic approach to fight against cybercrime. Some of the bills are highlighted below:

- There will be seven years jail term for offenders of different types of computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-squatting.
- Defines the liability of service providers and ensures that the use of electronic communications does not compromise national interest. It provides a legal framework to punish cyber criminals thereby improving electronic communication.
- It specifies all criminal acts and provides guidelines for the investigation of such offences. If these laws are effectively enforced, cybercriminals will be deterred and penalized. This will indirectly reduce the incident of cybercrimes, increase customer's confidence while transacting business online and also correct the negative impression about Nigeria and the citizens.

b) Individuals on their part should ensure proper security controls and make sure they install the latest security updates on their computer systems. In addition, they should observe the following (Lakshmi, 2015):

- Carefully select the sites you visit. Do not visit an untrusted site. Avoid visiting a site by clicking on a link you find in your email, found on a Facebook page, or on an advertisement
- Avoid pirated software and never disclose your Personal Identification Number (PIN), bank account and email access code to unknown persons.
- Always ignore any e-mail requiring your financial information. Do not send sensitive information in an email since its security cannot be guaranteed.
- Use strong passwords that are difficult to guess and employ a combination of characters (upper case and lowercase letters), numbers and symbols.
- Avoid inputting your information in a pop-up. If you have interest in any offer you see on a pop up, it is always safer to go directly to the website of the retailer.

3 Brief Analysis of Cybercrimes in Tertiary Institution in Ekiti State

The aim of this analysis is to evaluate the level of involvement of students in cybercrime and to determine their vulnerability in such crimes. This study adopts various research questions carried out among students in selected tertiary institutions in Ekiti-state. The research questions were distributed in the Federal University, Oye-Ekiti (FUOYE), Ekiti State University (EKSU) and finally Afe-Babalola University (ABUAD). Each institution is well populated; however, this study covers a total of 600 students from the combination of the three institutes between ages 15 to 26 years. These tertiary institutions were particularly selected as they cover all the types of tertiary institution, which includes state, federal and private universities, which an individual might attend. The questionnaire consisted of 15 questions that cuts across all the aspects of cybercrime in Nigeria especially within campuses. Each question had 5 options which includes:

- All the time (ATT)
- Most times (MT)
- Sometimes (ST)
- Seldom (SD)
- Never (NE)

From the options above, each student were to select one for every question given.

3.1 Results

The answers obtained from the questionnaires were analysed as discussed in this section. One of the questions asked during the survey was if the students possessed mobile phones and access to the internet since the internet is a main prerequisite for the manifestation of cybercrimes. The answer to this question formed the basis for other questions that were asked. It was observed from the answers to the questions that 96.8% of students have a mobile phone and also access to the internet.

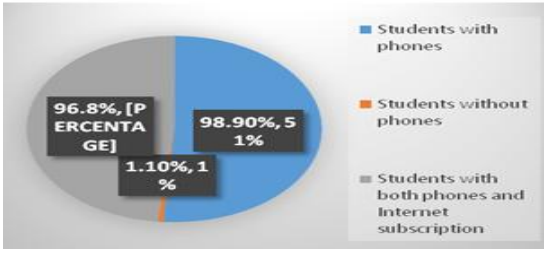
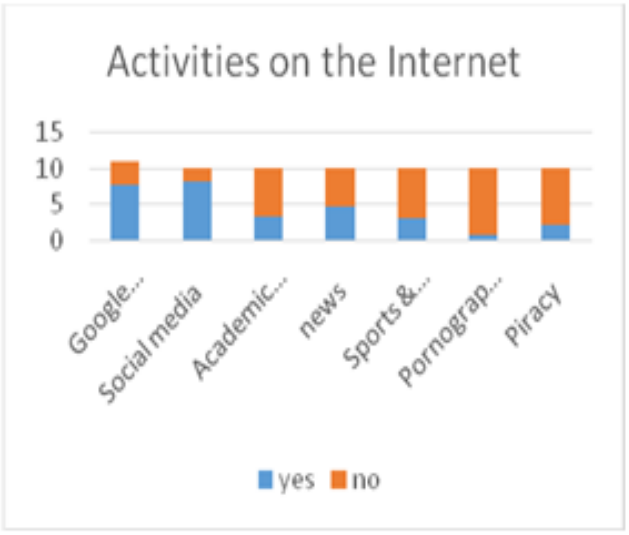


Fig 2. Possession of Phones accessible to the Internet

When asked about the activities that were mostly carried out using the internet either with a mobile phone, tablet or a laptop, the following responses were revealed and a conclusion made from the results that students spend more time on social media the most.

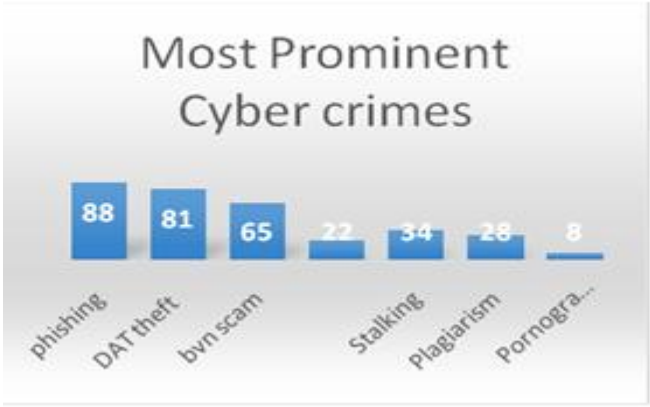


From the graph above, it shows that majority of the respondent's access google search (77%), social media (82%) and academic research (3.5%). While only few respondents use the internet for pornography (9%), sports and games (31%) and piracy (22%). It was found that respondents who access pornography are also involved in piracy and spamming while on the internet. The low response of the respondents was as a result of the sensitivity of the topic under study.

Views of Respondents on Places where Cyber Crime is perpetrated.

The graph above shows the points where cybercrimes are majorly performed. Findings reveal that 81% of the respondents agreed that cybercrimes are usually enacted at home and 80% said at school and then cybercafé.

Views of Respondents on which cybercrime is most prominent.



Furthermore, findings revealed that 88% of the students that participated in the analysis are victims of phishing. Majority said that they receive false mails and text messages which has in turn led to the loss of money and disclosure of private information in some cases. A close call to this crime carried out by students is the DAT Theft. According to the respondents, 81% have participated in this crime, referring to it as a "harmless" cybercrime.

4 Conclusion

Cybercrime is a menace that should be eradicated or reduced to a very minimal level for our great nation to break even. Several prominent cybercrimes and causes have been discussed in this paper. The study conducted in tertiary institutions in EkitiState to determine students' participation in cybercrimes shows that majority of the crimes conducted are carried out by the youths in our society majorly through phishing. Numerousways have been proposed to prevent future occurrence of this crime, however much can still be done by government and individuals to reduce it. It is recommended that our government should make the welfare and wellbeing of the citizens of paramount importance so as to lessen the burden of individuals by providing good paying jobs and other basic amenities. This will in no little way make life comfortable for people hence reduce their participation in criminal activities for survival. It is only after this is done that any bill or law against cybercrime can really take effect. Individuals are also enjoined to be smart and adhere to the preventive measures listed above in order not to fall victims. Moreover, since youths are the most involved in this crime, there is need for them to be orientated, educated and empowered for the country to have a greater future.

References

Hassan, A. B. Lass F. D. and Makinde J. (2012) *Cybercrime in Nigeria: Causes, Effects and the Way Out*, ARPN Journal of Science and Technology, vol. VOL. 2(7), 626 – 631.

Lakshmi P. andIshwarya M. (2015), *Cyber Crime: Prevention & Detection*," International Journal of Advanced Research in Computer and Communication Engineering, vol. Vol. 4(3).

Maitanmi, O. Ogunlere, S. andAyinde S. (2013), *Impact of Cyber Crimes on Nigerian Economy*, The International Journal of Engineering and Science (IJES, vol. vol 2(4), 45–51.

MichaelA.,Boniface., A. and Olumide, A. (2014) *Mitigating Cybercrime and Online Social Networks Threats in Nigeria*, Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz, vol. Vol I WCECS 2014, 22–24.

Ndible N., (2016*) Practical Application of Cyber Crime* Issues Retrieved on May 6, 2016 available at: http://ijma3.org/Admin/Additionals/Cybercrime/Nibal%20Idlebi%20Presentation.pdf

Shandilya A. (2011) *Online Banking: Security Issues for Online payment*,from www.buzzle.com/articles.

Okeshola F.B. and Adeta A.K, (2013) *The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria* American International Journal of Contemporary Research, vol. 3(9), 98-114.

Parthiban L. and Raghavan A. R. (2014), *The effect of cybercrime on a Bank's finances,* International journal of Current Research and Academic Review, vol. Volume-2(2), no. ISSN: 2347-3215, 173–178, Retrieved Feb. 2014 from www.ijcrar.com

Wada F. and Odulaja G. O. (2014), "Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation," Afr J Comp & ICT, Vol 4(3), no. Issue 2.

A Summary of the Legislation on Cybercrime in Nigeria, Legislative & Government Relations Unit, Public Affairs Deparment,Federal Bureau of Investigation (2016), ATM skimming,Retrieved June 8, 2016available online: https://www.fbi.gov/news/stories/2011/july/atm_071411.

Ewepu G, (2016) *Nigeria loses N127bn annually to cyber-crime* — NSA available at:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/Retrieved Jun. 9, 2016.

Iroegbu, *E "Cyber-security: Nigeria loses over N127bn annually through Cybercrime,"* available at: http://www.thisdaylive.com/index.php/2016/04/18/cyber-security-nigeria-loses-over-n127bn-annually-through-cybercrime/ Retrieved Jun. 9, 2016.

APPENDIX

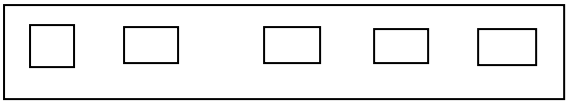
A. Evaluation: Questionnaire

Firstly, thank you for your time and agreeing to participate in this evaluation.

The aim of this research is to evaluate the level of awareness and involvement of students in cybercrime and to determine their vulnerability in such crimes. Each question has 5 options.From the options, you are to select one for every question given.

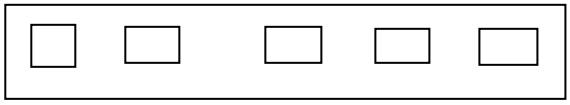
1. Do you possess a mobile phone?

All the time Most times Sometimes Seldom Never



2. Can you access the internet through your phone?

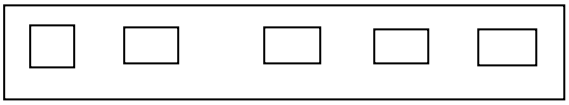
All the time Most times Sometimes Seldom Never



From questions 3-8, describe your level of involvement in the mentioned internet activity

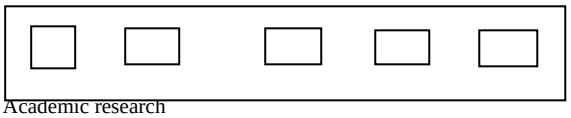
3. Google search

All the time Most times Sometimes Seldom Never



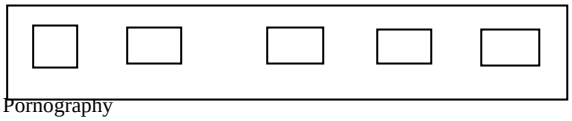
4. Social media

All the time Most times Sometimes Seldom Never



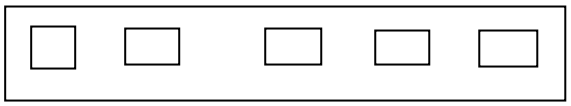
5. Academic research

All the time Most times Sometimes Seldom Never



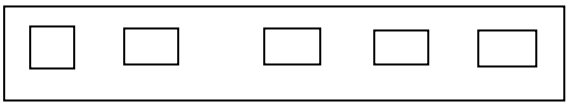
6. Pornography

All the time Most times Sometimes Seldom Never



7. Sports and games

All the time Most times Sometimes Seldom Never



8. Piracy

All the time Most times Sometimes Seldom Never